04-10-00

A

04/07/00 JC712 U.S. PTO

JC511 U.S. PTO 09/545381 04/07/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventors: SPIELMANN, Craig
HUTTER, Maria
KLEIN, Joel
SINGHANI, Naresh

Filed: Herewith

Title: Method And System For Managing Risks

Attorney Docket No. JPM-001

CERTIFICATE OF MAILING UNDER 37 CFR § 1.10
"Express Mail" Mailing Label Number

EL 577174616US

Date of Deposit: April 7, 2000

I hereby certify that this paper and all enclosures referred to therein are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above with sufficient postage in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Name of Person Mailing: Meredith R. Taylor

Meredith Taylor
Signature of Person Mailing

09545381.040700

PATENT APPLICATION TRANSMITTAL LETTER

Assistant Commissioner for Patents
BOX PATENT APPLICATION
Washington, D.C. 20231

Sir:

Transmitted herewith are the following:

Specification, including claims, abstract and ten figures (37 pages),

Combined Declaration and Power of Attorney

Return receipt postcard.

09545381 .040700

Fees

				SMALL ENTITY		OTHER	
				Rate	Fee	Rate	Fee
Basic Fee					$		$ 690.00
Total Claims	18			x 9.00	$	x 18.00	$
Indep. Claims	4			x 39.00	$	x 78.00	$ 78.00
Multiple Dependent Claim(s):					$ 0		$
				TOTAL:	$	TOTAL	$ 729.00

The Commissioner is hereby authorized to charge the filing fee and any fees which may be required in connection with this submission, to **Deposit Account No. 19-2385**. (Please reference attorney docket no. JPM-001).

Date: April 7, 2000

Respectfully submitted,

By:____________________
Andrew Strobert
Registration No. 35,375
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Four Times Square
New York, New York 10022
(212) 735-3000

METHOD AND SYSTEM FOR MANAGING RISKS

Field of the Invention

The present invention relates to a method and system for managing risks inherent in business activities and more particularly to a data processing apparatus and method for identifying, managing and quantifying risks and associated control procedures.

Background of the Invention

Many organizations worldwide have developed practices for internal control. The Institute of Internal Auditors' ("IIA") Standards for the Professional Practice of Internal Auditing (Standards) defines control as:

> ...any action taken by management to enhance the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. (Section 300.06)

According to Specific Standard 300.05, the primary objectives of internal control are to ensure:

1. The reliability and integrity of information.
2. Compliance with policies, plans, procedures, laws, regulations, and contracts.
3. The safeguarding of assets.

4. The economical and efficient use of resources.

5. The accomplishment of established objectives and goals for operations or programs.

Many organizations have recognized the need for tracking the effectiveness of internal control practices. For example, according to the IIA's Professional Practices Pamphlet 97-2, Assessing and Reporting on Internal Control, the IIA supports the Committee of Sponsoring Organizations of the Treadway Commission, recommendation that organizations should report on the effectiveness and efficiency of the system of internal control.

One system of internal control, the Control Self-Assessment (CSA) methodology, was initially developed in approximately 1987 and is used by many organizations to review key business objectives, risks involved in achieving objectives, and internal controls designed to manage those risks. The IIA states that some CSA proponents have expanded this description to encompass potential opportunities as well as risks, strengths as well as weaknesses, and the overall effectiveness of the system in ensuring that the organization's objectives are met.

CSA approaches and formats may differ from one organization to another, however, the three primary CSA approaches are: facilitated team meetings (also known as workshops), questionnaires and management-produced analysis. Organizations may combine more than one approach. Facilitated team meetings gather internal control information from work teams that may represent multiple levels within an organization. The questionnaire approach uses a survey instrument that offers opportunities for simple yes/no or have/have not responses. Management-produced analysis is any approach that does not use a facilitated meeting or survey.

While existing methodologies and systems, such as the CSA, offer some structure in approaching the control of risk, to date, no system or methodology known to the applicants exists that properly quantities risks and the effectiveness of control procedures designed to address such risks. For example, many existing systems rely on a single weak link approach, without consideration of the significance of such link. If an assessor utilizing the weak link approach identifies a large number of processes associated with a risk element (e.g. business continuity), the presence of a single non-complaint process would red-flag the entire risk element, regardless of the significance of the non-complaint process. Thus, existing systems provide no mechanism for comparing results over time, nor are they reliable for providing a meaningful index of how well individual entities are measuring risk.

The method and system of the present invention addresses these and other limitations by utilizing a quantative weighted approach to evaluating risk. A threetiered approach to evaluate risk is preferably used, dividing the system into: "Risks", "Subrisks," and "Control Procedures." An assessor is prompted through a series of screens to rate risks as "High," "Medium" and "Low." At the next level (the "Subrisk" level), a set of control procedures is provided. Each control procedure is rated by the assessor according to a number of categories, such as GREEN (full compliance), YELLOW (partial compliance), RED (non-compliance), or BLUE (not applicable). Control Procedures are assigned different weights because some risks are more critical than others. For items which are not fully compliant (e.g. items rated either YELLOW (partial compliance) or RED (non-compliance)), the assessor must either indicate that the risk is acceptable or create an action plan where deliverables are identified and target dates are established.

The system further provides a method of weighing, sorting and graphing displays which allows management to more easily identify significant areas of risk. This allows assessors to sort and view data in a number of ways, such as toy organization, business line, city and process. The display system further allows the user to "drill down" by clicking on high risk areas facilitating the identification of specific assessments which are having a significant impact on the risk rating.

Targets are derived from the Action Plans. A target is an index or measure which informs management of progress against action plans. Targets and actual results will be compared from quarter to quarter, to determine whether appropriate progress is being made against commitments.

Brief Description of the Figures

These and other aspects of the present invention are more apparent in the following detailed description and claims, particularly when considered in conjunction with the accompanying drawings showing a system constructed in accordance with the present invention, in which:

Figure 1 is a system diagram showing the components of an exemplary system implementing the present invention;

Figures 2 is a logic diagram showing a preferred embodiment of the risk management system of the present invention;

Figure 3 is an exemplary computer display for rating the importance of a set of risk elements;

Figure 4 is an exemplary computer display showing subrisks, control procedures, compliance ratings and an action plan for non-fully complaint risks;

Figure 5 is an exemplary computer display for accepting risks or entering action plans;

Figure 6 is an exemplary computer display showing overall compliance scores sorted by business process;

Figure 7 is an exemplary computer display showing compliance scores for a specific subrisk sorted by city;

Figure 8 is an exemplary computer display showing a forecast report sorted by city and subrisk;

Figure 9 is an exemplary computer display showing actual versus target compliance scores sorted by subrisk; and

Figure 10 is an exemplary computer display showing an action plan count sorted by process and city.

Detailed Description of the Invention

Figure 1 depicts the components of an exemplary computing system implementing the inventive system for managing risk. Server 101 includes one or more communications ports 109 for communicating with assessors utilizing client workstations 108. Server 101 is coupled to one or more storage devices 103. Storage device(s) 103 include an executable or interpretable program 104 for controlling the management system. Storage device(s) 103 also include a rating database 105 containing data elements necessary for the rating process, and a quarterly assessment database 106 containing data elements necessary for quarterly assessments.

Figure 2 presents an overview of the inventive process of categorizing, weighing and tracking risks. Initially, a set of risk elements are identified 201. The following are exemplary risks in the field of investment management: (i) Business continuity, (ii) Financial, (iii) Information, (iv) Legal/Regulatory, (v) People, (vi) Physical Security, and (vii) Technology, however the set of risk elements will vary from application to application. Each risk is rated 202 preferably according to a fixed set of criteria. In the preferred embodiment of the invention these criteria comprise the probability of occurrence and the impact to the business should the situation occur. Each risk is also preferably rated by a fixed set of rankings, such as "High," "Medium" and "Low." Figure 3 is an exemplary computer display showing the rating 301 of risk elements 302 as High, Medium or Low. Each of these ratings 301 is stored in rating database 105 with the associated risk elements 302. Although not used in the preferred embodiment of this invention, these criteria and rankings may optionally be used in the weighing formula discussed below.

Each subrisk of the risk elements is identified 203 and presented to the user. In the preferred embodiment, these subrisks comprise:

1. Business Resumption:
   i. Business Resumption; and
   ii. Viruses.
2. Financial:
   i. Expense Management.

3. Information:
    - i. Restoration; and
    - ii. Security.
4. Legal/Regulatory:
    - i. Vendor Management; and
    - ii. Software Licensing.
5. People:
    - i. Capabilities; and
    - ii. Compliance.
6. Physical Security:
    - i. Physical access.
7. Technology:
    - i. Change management;
    - ii. Problem management;
    - iii. Strategy; and
    - iv. Dependability

Figure 4 is an exemplary computer display showing the display of the subrisks, Business Resumption and Viruses 402A & 402B, identified in the preferred embodiment for the Business Resumption risk 401.

One or more control procedures for each sub-element are then identified 204 and displayed to the user. In the preferred embodiment, these control procedures comprise:

Risk: 1. Business Continuity
    Subrisks:
        i. Business Resumption:
        Control Procedures:
            a. Change Management;
            b. Management Reporting;
            c. Off-site Recovability;
            d. Test Performance; and

e. Testing.

ii. Viruses

Control Procedures:

a. Anti-virus Software;
b. Currency of Anti-virus Software;
c. Scanning Practices; and
d. Scope of Scanning.

2. Financial

Subrisks:

i. Expense Management:

Control Procedures:

a. Detailed budget;
b. Expenditure vs. plan; and
c. Expense Management Report.

3. Information

Subrisks:

i. Restoration

Control Procedures:

a. Data back-up requirements;
b. Media worthiness;
c. Off-site storage;
d. Back-up performances; and
e. Back-up testing.

ii. Security

Control Procedures:

a. Security awareness;
b. Data guardian;
c. User ID administration;
d. Rectification;
e. User termination procedures;
f. Violation monitoring;
g. Dial-up access;
h. Adherence to standards;
i. Access approval process;
j. Testing;
k. User time-out; and
l. Data encryption.

4. Legal/Regulatory

Subrisks:

- i. Vendor Management

  Control Procedures:

  - a. Legal counsel;
  - b. Escape clauses;
  - c. Audit clauses;
  - d. Adherence to policies;
  - e. Point person established;
  - f. Escalation process;
  - g. Billing reconciliation; and
  - h. Performance reporting.

- ii. Software Licensing

  Control Procedures:

  - a. Awareness;
  - b. Software inventory;
  - c. Documentation;
  - d. Upgrade documentation;
  - e. Compliance testing;
  - f. Invoices; and
  - g. Entitlements - market data access is assigned to users based on contractual agreements.

5. People

Subrisks:

- i. Capability

  Control Procedures:

  - a. Sourcing Strategy;
  - b. Staff Retention;
  - c. Succession Plans;
  - d. Recruiting;
  - e. Performance evaluations; and
  - f. Attrition.

- i. Compliance

  Control Procedures:

  - a. Diversity;
  - b. Core Values;
  - c. JPM work authorization;

d. Adherence to policies; and
e. Policy Review.

6. Physical Security
Subrisks:

i. Capability
Control Procedures:

a. Location Security;
b. Restricted Access;
c. Recertification;
d. Termination process;
e. Environment controls; and
f. Power supply.

6. Technology
Subrisks:

i. Change Management
Control Procedures:

a. Documented Process;
b. Process Compliance;
c. Testing Changes;
d. Business Communication;
e. Change Integrity;
f. Emergency Change Approval;
g. Planning & Scheduling;
h. Offsite Change Coordination;
i. Back out;
j. Segregation of Duties; and
k. Business Impact.

ii. Problem management
Control Procedures:

a. Documented Process;
b. Monitoring and Alerts;
c. Help Desk;
d. Problem reporting process;
e. Trend Analysis; and
f. Problem resolution.

iii. Strategy

Control Procedures:

a. Business Plans;
b. Business Sponsorship;
c. Strategy Alignment;
d. Strategy Communication;
e. Project Marketing;
f. Service Level Agreements;
g. Project Management; and
h. Management Reporting.

iv. Dependability

Control Procedures:

a. Adherence Standards;
b. Performance Monitoring;
c. Service Level Agreements;
d. Management Reporting;
e. Capacity Planning;
f. Hardware Reliability;
g. Hardware Refresh;
h. Software Currency;
i. Level of business impact;
j. Assets Inventory;
k. Redundancy; and
l. Y2K Compliance.

Figure 4 shows the display of the control procedures 403A - 403E for the Business Resumption subrisk 402A. The user is provided with a detailed description 404 of each control procedure by selecting one of the descriptive terms 403A - 403E listed under the associated subrisk.

Each control procedure is assigned 205 a weight or control procedure priority ("CP-priority"). In the preferred embodiment, the following CP-priorities are used: very high=10, high=7, medium=4 and low=1. Each assigned CP-priority is stored in the rating database 105. Priorities for control procedures are preferably pre-set by an administrator.

The user is prompted to enter (see 405, Figure 4) a compliance rating for each control procedure 206. In the preferred embodiment, these ratings comprise: green=full compliance, yellow=partial compliance, red=non-compliance, and blue=not applicable. For each non-compliance or partial compliance control procedure, the user will be prompted 501 (Figure 5) to determine 208 whether to enter an action plan or accept the risk. For each action plan created 209, the user will enter a description 502, target date 503 and additional comments 504. The user may also enter an estimated cost 505 and assign individuals 506 to the action plan.

In the preferred embodiment, each assessor also associates a number of additional parameters with each subrisk and/or control procedure. For example, the assessor may associate a process, city or region, or organization with each entry. Other parameters would be apparent in other applications. This associated data is stored in the rating database 106 and may be used for sorting and displaying as discussed below.

The compliance score is preferably based on cumulative weighting of two factors: the priority weight of each control procedure ("CP_weight") and the compliance or status factor ("CP_status_factor") for each such control procedure. In the preferred embodiment, this is calculated as:

Subrisk score equals:

$\sum_{\text{control procedures}} ((\text{CP\_weight} / (\sum_{\text{control procedures}} (\text{CP\_weight})) * \text{CP\_status\_factor}) * 10$,

and the overall score equals the average of all the subrisk scores.

where:

$\sum_{\text{control procedures}}$ sums the control procedures for a given subrisk.

CP_weight ranges from:

status	weight
extremely high	scaleable (i.e. 10)
high	scaleable (i.e. 7)
medium	scaleable (i.e. 4)
low	scaleable (i.e. 1)

CP_status_factors range from:

status	weight
full compliance(green)	scaleable (i.e. 10)
partial compliance(yellow)	scaleable (i.e. 4)
non-compliance(red)	scaleable (i.e. 1)
not applicable (blue)	scaleable (i.e. 0)

An example implementation of this scoring system is given in Table I below:

TABLE I

CP_Priority	CPP Weight

Extr. High	(EH)	1.8
High	(H)	1.1
Med.	(M)	1
Low	(L)	0.5

Status		Factor
Green	(G)	10
Yellow	(Y)	6
Red	(R)	2
Blue	(B)	0

scoring

Subrisk A	CP	Priority	Weight	Status	Status Factor	Weight %	Status factor x weight%	
	A	EH	1.8	G	10	33%	3.33	
	B	H	1.1	R	2	20%	0.41	
	C	M	1	Y	6	19%	1.11	
	D	M	1	G	10	19%	1.85	
	E	L	0.5	R	2	9%	0.19	
	F	M	0	B	0			
			Total Weight			100%	6.89	Add up scores
			5.4				68.89	Total score x 10

scoring

Subrisk B	CP	Priority	Weight	Status	Status Factor	Weight %	Status factor x weight%
	G	EH	1.8	R	2	46%	0.92
	H	H	1.1	R	2	28%	0.56

I	L	0.5	G	10	13%	1.28	
J	L	0.5	G	10	13%	1.28	
		Total Weight					
		3.9			100%	4.05	Add up scores
						40.51	Total score x 10

scoring

Subrisk C	CP	Priority	Weight	Status	Status Factor	Weight %	Status factor x weight%	
	K	EH	1.8	R	2	32%	0.63	
	L	EH	1.8	G	10	32%	3.16	
	M	EH	0.5	G	10	9%	0.88	
	N	L	0.5	Y	6	9%	0.53	
	O	M	0	B	0	0%	0.00	
	P	M	0	B	0	0%	0.00	
	Q	H	1.1	G	10	19%	1.93	
			Total Weight			100%	7.12	Add up scores
			5.7				71.23	Total score x 10

09545361.040700

Overall Score

	score
Subrisk A	68.89

Subrisk B			40.51		
Subrisk C			71.23		
	Total Weight	180.63	Divide by # of Sub-risks (e.g. 3)	180.6/3	60.21

Based on the target dates set in the action plans, the system may also optionally calculate 210 future compliance scores. This allows assessors to easily determine whether action plans are aggressive enough or unnecessarily aggressive. This also allows administrators to create a simple metric for determining how well groups perform in meeting their action plans.

The novel system of weighing and categorizing risk of the present invention also facilitates the display of risk data in a number of ways which heretofore had not been possible. For example, compliance scores may be sorted by process (e.g., voice, desktop, midrange, networks, mainframe, market data, etc.) and displayed as shown in Figure 6. As a further example, Figure 7 shows compliance scores for individual subrisks sorted by business location. Various other ways of sorting and displaying compliance scores will be apparent to those of skill in the art and include, for example, compliance scores for individual processes sorted by business organization, or compliance scores for individual business organizations sorted by business location. Such displays are extremely helpful to management in locating weak spots in risk compliance.

The system of the present invention also facilitates the ability to predict future levels of compliance and to teach entities ability to meet forecasts. Forecasts versus actual results may be sorted in any of a number of ways. Figure 8 shows the forecast versus actual results for an individual city and individual subrisk. As shown in Figure 9, actual versus target results may be sorted by subrisk and displayed.

Figure 10 shows an action plan status report for an individual process and individual city. Other reports made possible by the system of the present invention will be understood by those of skill in the art, and include, for example, views showing the number of compliant and non-compliant control procedures sorted by accessing organization.

Although the specification and illustrations of the invention contain many particulars, these should not be construed as limiting the scope of the invention but as merely providing an illustration of the preferred embodiments of the invention. For example, while the system is described in terms of risks and subrisks, it will be understood by those of ordinary skill in the art based on the specification herein that the method and system may be utilized using a single category of risks. Moreover, while the described system is described in terms of identifying one or more control procedures for each subrisk element, it will also be understood by those of ordinary still in the art, based on the specification herein, that the system may be designed to allow assessors to identify non-applicable subrisks in which case it would be unnecessary to identify control procedures for such subrisks. Thus, the claims should be construed as encompassing all features of patentable novelty that reside in the present invention, including all features that would be treated as equivalents by those skilled in the art.

What is claimed is:

1. A method of managing risk with the aid of a computer system, said method comprising:

a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;

b. identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;

c. assigning a weight to each said control procedure;

d. determining a compliance rating for each said control procedure; and

e. calculating a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures.

2. The method of claim 1, wherein said compliance ratings comprise at least one rating identifying a non-fully compliant control procedure, said method further comprising the steps of:

a. for each said control procedure having a non-fully compliant rating, receiving a signal indicating whether said non-fully compliant rating is accepted or not accepted; and

b. for each said non-fully compliant control procedure which is indicated as not accepted, generating an action plan.

3. The method of claim 2 wherein said action plan include a target date, said method further comprising the step of calculating an expected compliance score for one or more future dates based on said action plan target dates.

4. The method of claim 3 further comprising the step of tracking whether said expected compliance scores have been met, said tracking including calculating actual compliance scores for said target dates.

5. The method of claim 4 further comprising the step of displaying said expected compliance scores versus said actual compliance for said target dates.

6. The method of claim 1 further comprising the step of associating one or more parameters with each said compliance rating.

7. The method of claim 6 wherein said one or more parameters are selected from the group comprising organization, business line, process, and region.

8. The method of claim 6 further comprising the step of sorting said compliance scores by said one or more parameters.

9. The method of claim 8 further comprising the step of displaying said sorted compliance scores.

10. A method of managing risk with the aid of a computer system, said method comprising:

a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;

b. identifying one or more subrisk elements associated with each said risk element, each said subrisk element being stored in said database;

c. identifying one or more control procedures associated with each said subrisk element, said control procedures being stored in said database;

d. assigning a weight to each said control procedure;

e. determining a compliance rating for each said control procedure, said compliance ratings including a plurality of categories including at least one category indicating said control procedure is not fully compliant;

f. calculating a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures;

g. for each said subrisk, determining whether at least one control procedures associated with said subrisk is not fully compliant;

h. for each said subrisk associated with at least one control procedure which is not fully compliant, receiving a signal indicating whether said subrisk should be accepted or not accepted; and

i. for each said subrisk which is indicated as not accepted, generating an action plan.

11. The method of claim 10 wherein said action plan further includes a target date, said method further comprising the step of calculating a future compliance score based on said action plan target dates.

12. The method of claim 10 further comprising the step of associating one or more parameters with each said compliance rating.

13. The method of claim 12 further comprising the step of sorting said compliance ratings and displaying said sorted ratings.

14. A method of forecasting risk with the aid of a computer system, said method comprising:

a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;

b. identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;

c. assigning a weight to each said control procedure;

d. determining a compliance rating for each said control procedure, said compliance ratings chosen from a set of ratings including at least one rating identifying a non-fully compliant control procedure and at least one rating identifying fully compliant control procedures;

e. for each said control procedure having a non-fully compliant rating, generating an action plan, said action plan including a target date for at least one action listed therein; and

f. calculating an expected compliance score for a future date, said expected compliance score being a function of said assigned weights, said fully compliant control procedures, and said action plan target dates for said non-fully compliant control procedures.

15. The method of claim 14 wherein said action plan comprises a signal indicating whether said non-fully compliant rating is accepted or not accepted, said expected compliance score further being a function of said non-fully compliant ratings which have been accepted.

16. A data processing system for managing risk, said system comprising:

a. a database;

b. a processor coupled to said database, said processor being programmed to perform the steps comprising:

i. receiving a first signal identifying a set of risk elements, said risk elements being stored in said database;

ii. receive a second signal identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;

iii. receive a third signal assigning a weight to each said control procedure, said weight being stored in said database;

iv. receive a fourth signal identifying a compliance rating for each said control procedure; and

v. calculate a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures.

17. The data processing system of claim 16, wherein said compliance ratings comprise at least one rating identifying a non-fully compliant control procedure, said processor being further programmed to perform the steps comprising:

a. for each said control procedure having a non-fully compliant rating, receiving a signal indicating whether said non-fully compliant rating is accepted or not accepted;

b. for each said non-fully compliant control procedure which is indicated as not accepted, receiving an action plan, said action plan including an expected target date for implementation and an expected compliance rating; and

c. generating one or more future expected compliance scores, said compliance scores being a function of said target dates, said assigned weights and said expected compliance rating of said control procedures.

18. The data processing system of claim 16 further comprising a computer display coupled to said processor, said processor further being programmed to display said compliance scores on said computer display.

ABSTRACT

A data processing system and method of using said data processing system for assessing and managing risk is disclosed. The preferred embodiment of the method includes the steps of identifying a set of risk elements; determining an importance for each said risk element; identifying any subrisks associated with said risk elements; identifying one ore more control procedures for each said subrisk element; assigning weights to each said control procedure; rating compliance with each said control procedure and calculating an overall weighed compliance score. The method may further include the steps of for each non-fully compliant subrisk, allowing the user to determine whether to accept the risk or generate an action plan addressing the risk. The method may further preferably include calculating future compliance scores based on said action plans. The system further provides for sorting and displaying compliance scores by a number of parameters.

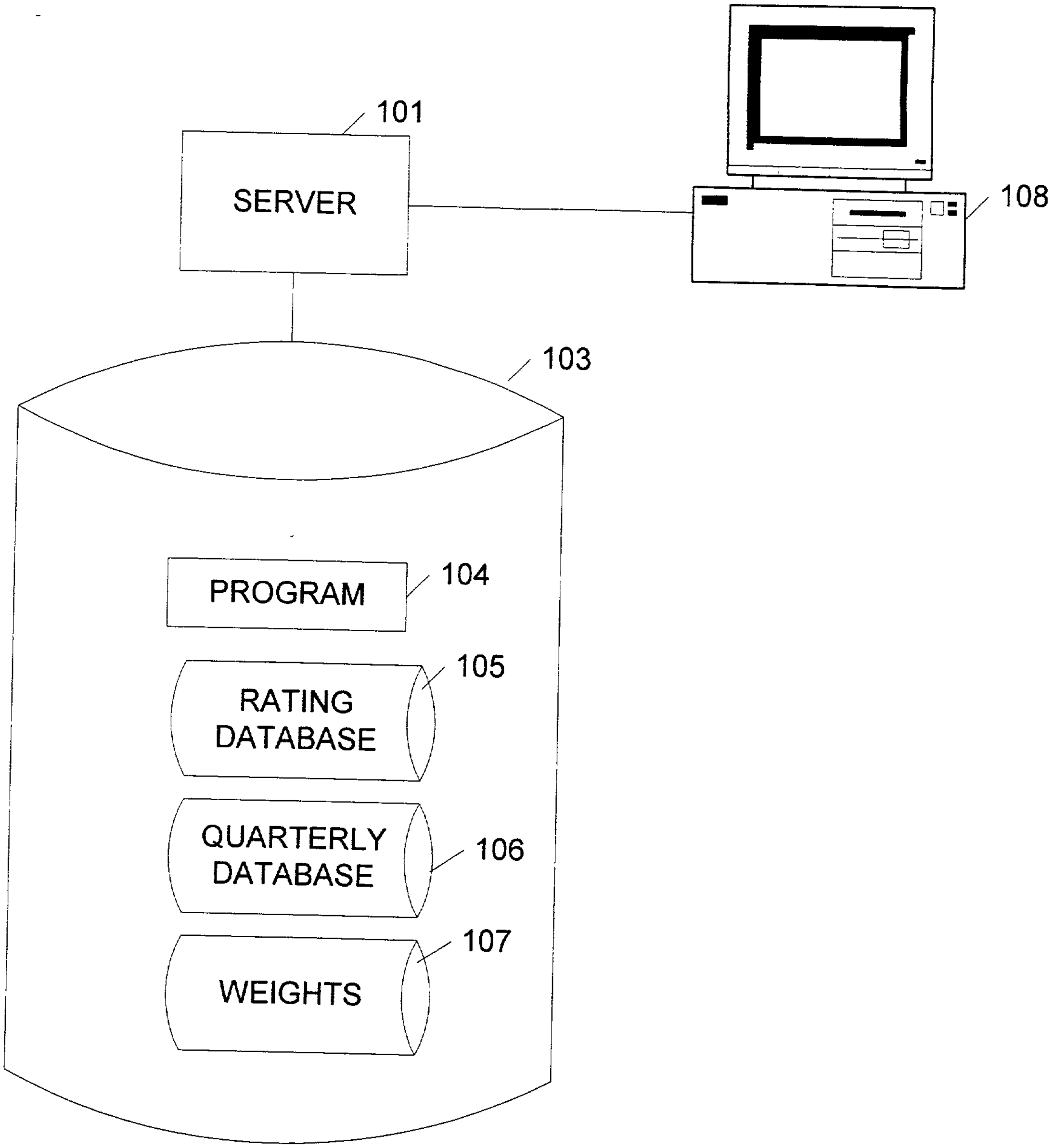
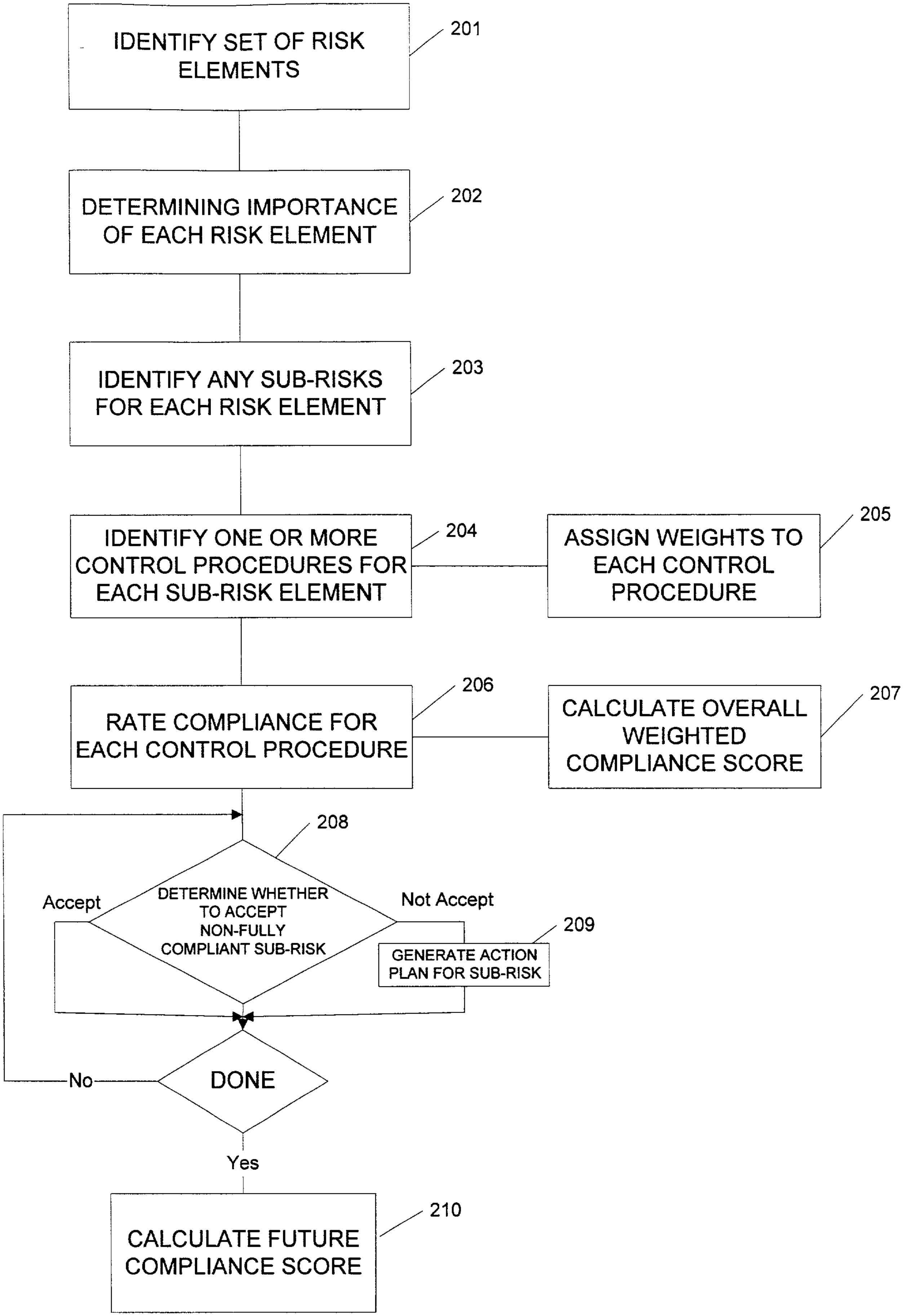
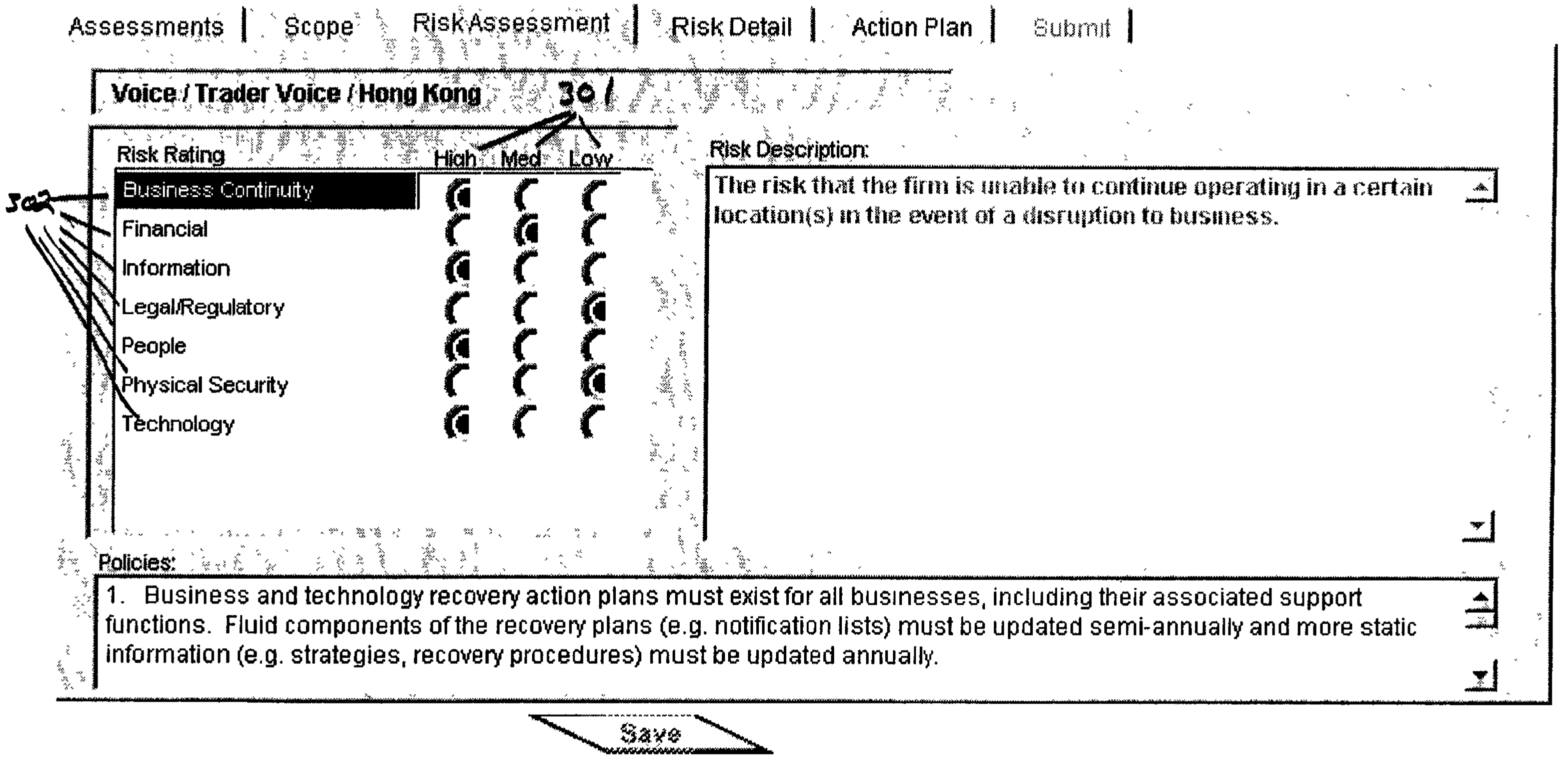


FIGURE 1

09545183.040200

Figure 2


IDENTIFY SET OF RISK ELEMENTS
201
DETERMINING IMPORTANCE OF EACH RISK ELEMENT
202
IDENTIFY ANY SUB-RISKS FOR EACH RISK ELEMENT
203
IDENTIFY ONE OR MORE CONTROL PROCEDURES FOR EACH SUB-RISK ELEMENT
204
ASSIGN WEIGHTS TO EACH CONTROL PROCEDURE
205
RATE COMPLIANCE FOR EACH CONTROL PROCEDURE
206
CALCULATE OVERALL WEIGHTED COMPLIANCE SCORE
207
208
DETERMINE WHETHER TO ACCEPT NON-FULLY COMPLIANT SUB-RISK
Accept
Not Accept
GENERATE ACTION PLAN FOR SUB-RISK
209
DONE
No
Yes
CALCULATE FUTURE COMPLIANCE SCORE
210



Voice / Trader Voice / Hong Kong

Risk Rating	High	Med	Low
Business Continuity	●	○	○
Financial	○	●	○
Information	●	○	○
Legal/Regulatory	○	○	●
People	●	○	○
Physical Security	○	○	●
Technology	●	○	○

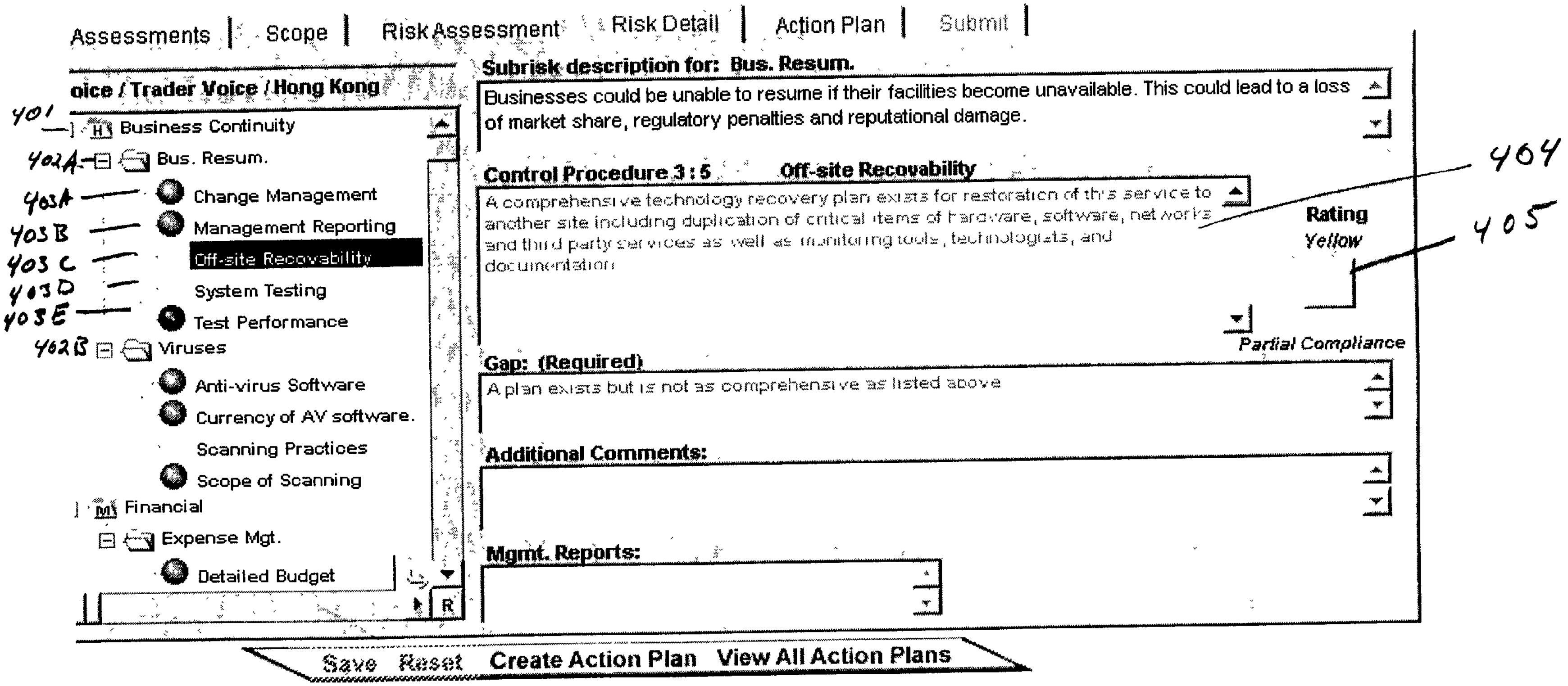
Risk Description:

The risk that the firm is unable to continue operating in a certain location(s) in the event of a disruption to business.

Policies:

1. Business and technology recovery action plans must exist for all businesses, including their associated support functions. Fluid components of the recovery plans (e.g. notification lists) must be updated semi-annually and more static information (e.g. strategies, recovery procedures) must be updated annually.

FIGURE 3



Subrisk description for: Bus. Resum.

Businesses could be unable to resume if their facilities become unavailable. This could lead to a loss of market share, regulatory penalties and reputational damage.

Control Procedure 3 : 5 **Off-site Recovability**

A comprehensive technology recovery plan exists for restoration of this service to another site including duplication of critical items of hardware, software, networks and third party services as well as monitoring tools, technologists, and documentation

Rating
Yellow

Partial Compliance

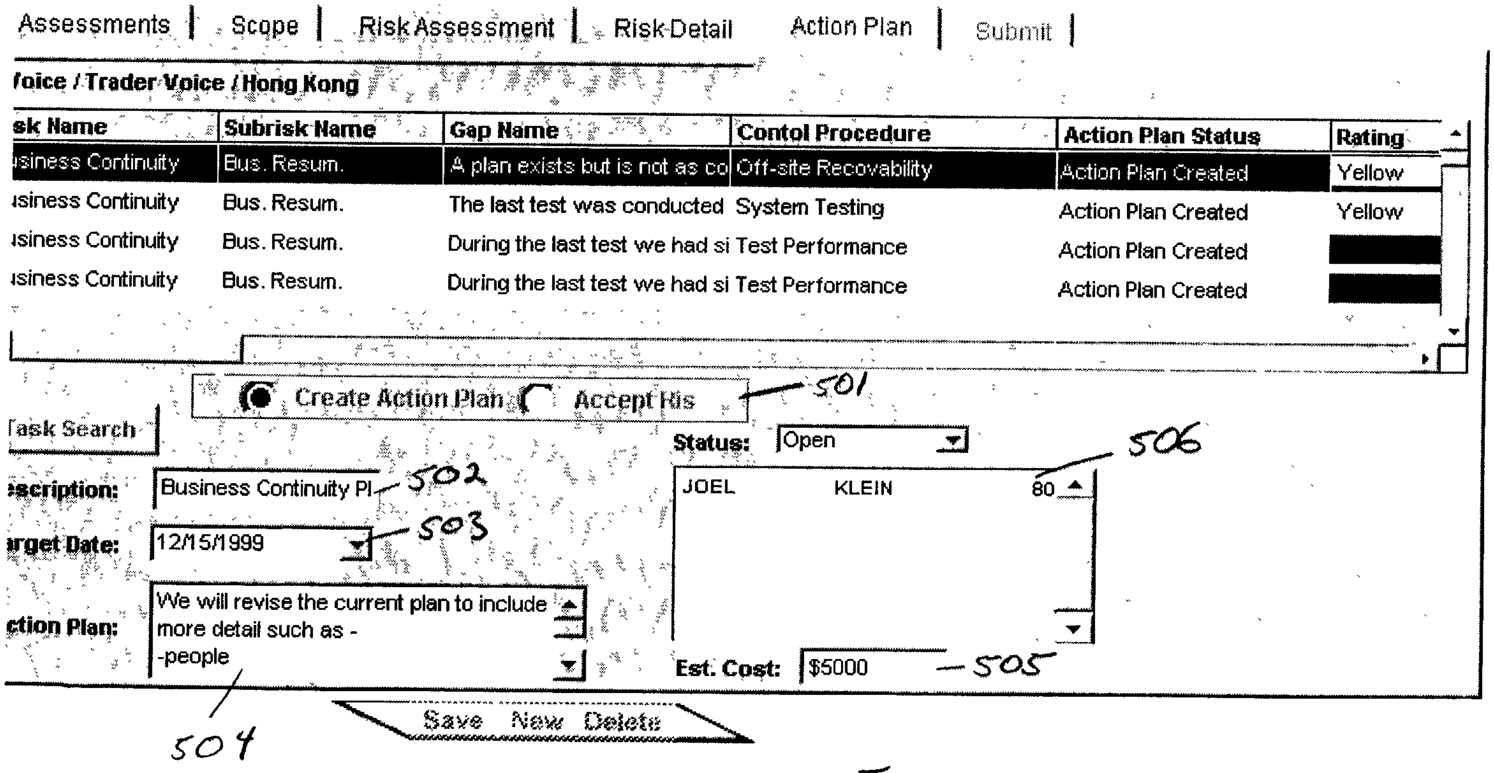
Gap: (Required)

A plan exists but is not as comprehensive as listed above

Additional Comments:

Mgmt. Reports:

FIGURE 4



Assessments | Scope | Risk Assessment | Risk Detail | Action Plan | Submit |

/oice / Trader Voice / Hong Kong

sk Name	Subrisk Name	Gap Name	Contol Procedure	Action Plan Status	Rating
ısiness Continuity	Bus. Resum.	A plan exists but is not as co	Off-site Recovability	Action Plan Created	Yellow
ısiness Continuity	Bus. Resum.	The last test was conducted	System Testing	Action Plan Created	Yellow
ısiness Continuity	Bus. Resum.	During the last test we had si	Test Performance	Action Plan Created	■
ısiness Continuity	Bus. Resum.	During the last test we had si	Test Performance	Action Plan Created	■

● Create Action Plan ○ Accept Ris

Task Search

escription: Business Continuity Pl

arget Date: 12/15/1999

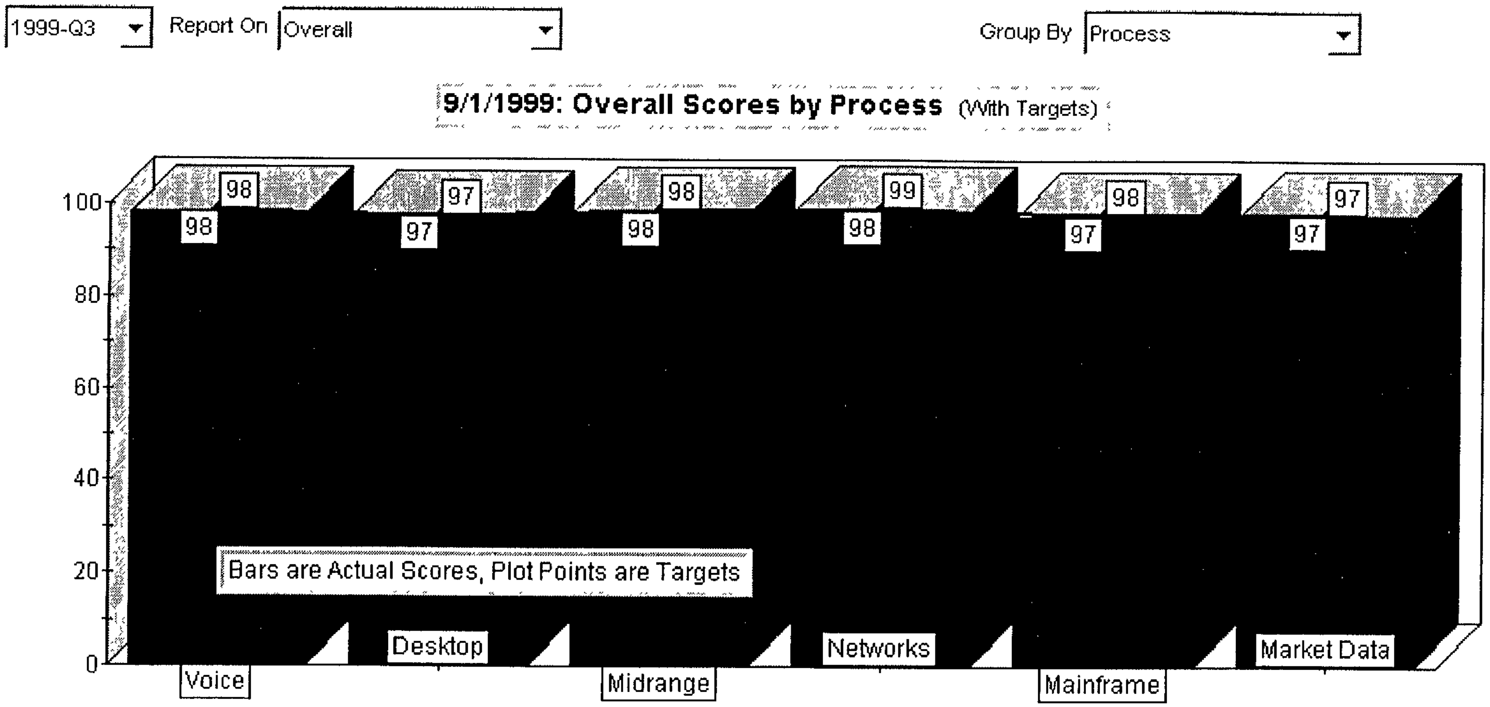
ction Plan: We will revise the current plan to include more detail such as -
-people

Status: Open

JOEL	KLEIN	80

Est. Cost: $5000

FIGURE 5

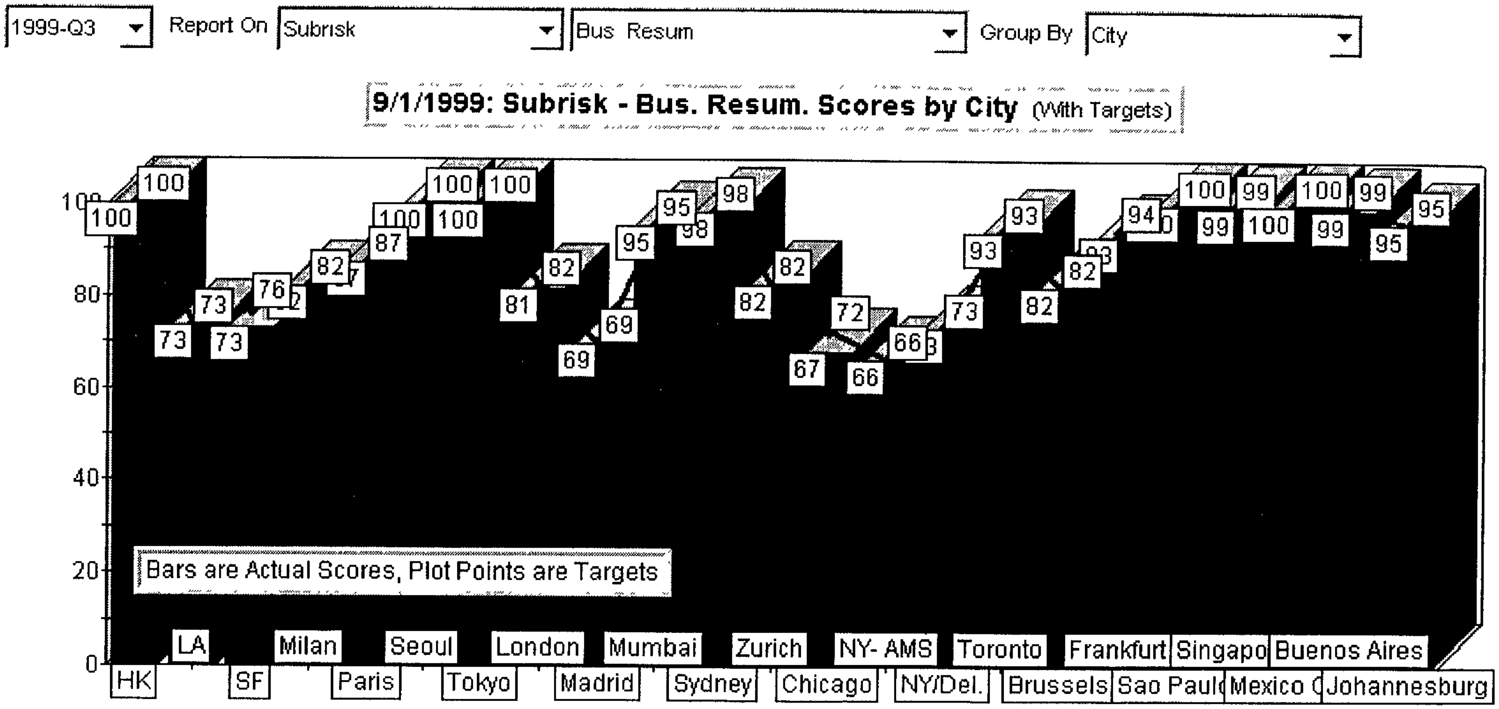


1999-Q3 ▼ Report On Overall ▼ Group By Process ▼

9/1/1999: Overall Scores by Process (With Targets)

Bars are Actual Scores, Plot Points are Targets

FIGURE 7

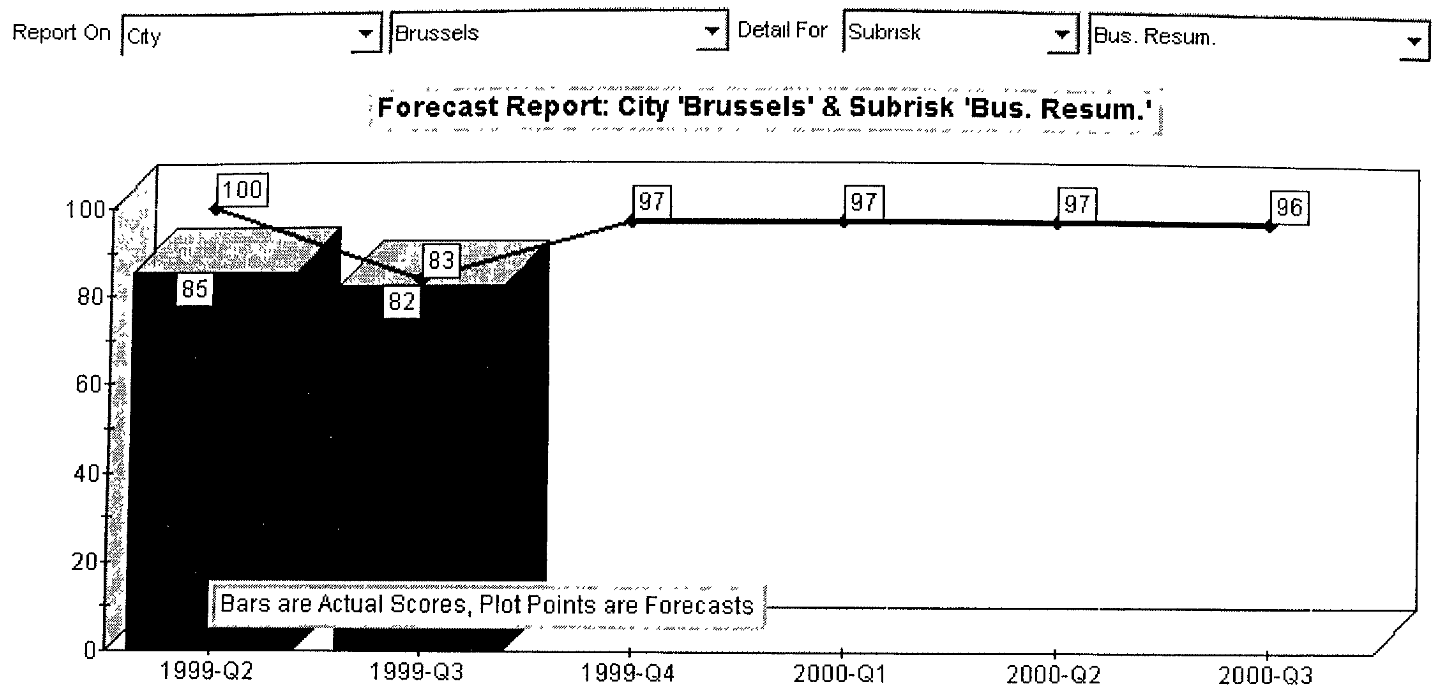


1999-Q3 ▼ Report On Subrisk ▼ Bus Resum ▼ Group By City ▼

9/1/1999: Subrisk - Bus. Resum. Scores by City (With Targets)

Bars are Actual Scores, Plot Points are Targets

Figure 8

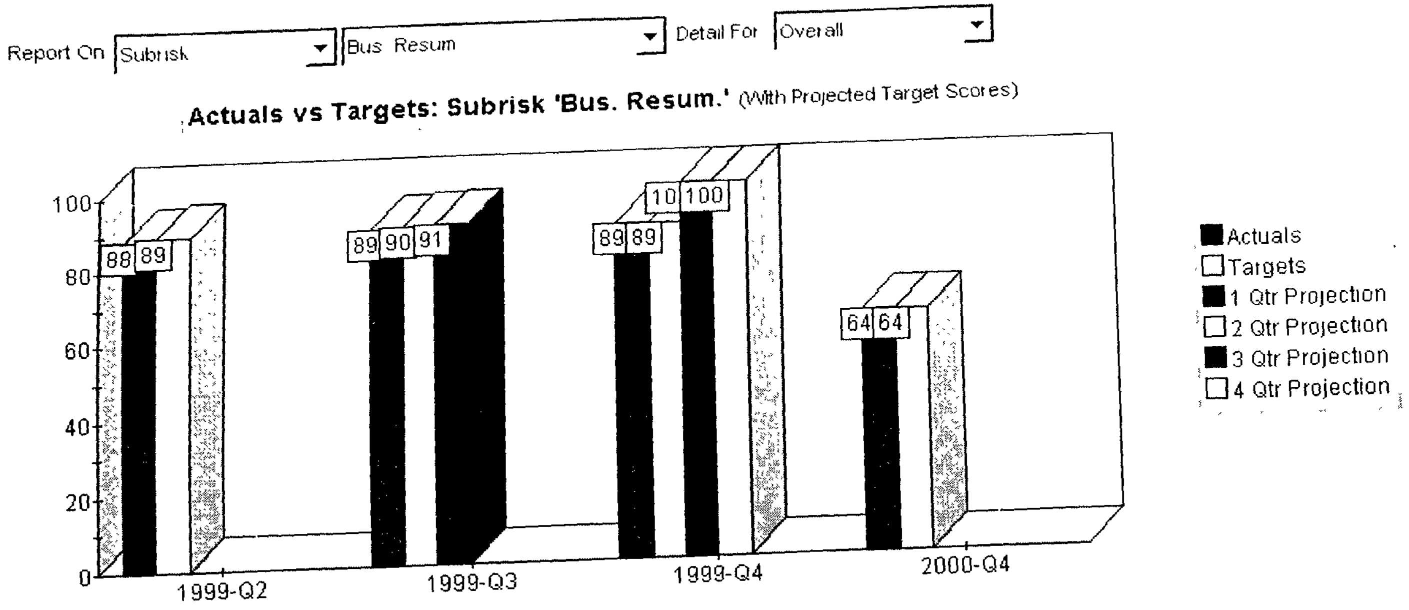


Report On: City | Brussels

Detail For: Subrisk | Bus. Resum.

Forecast Report: City 'Brussels' & Subrisk 'Bus. Resum.'

FIGURE 9

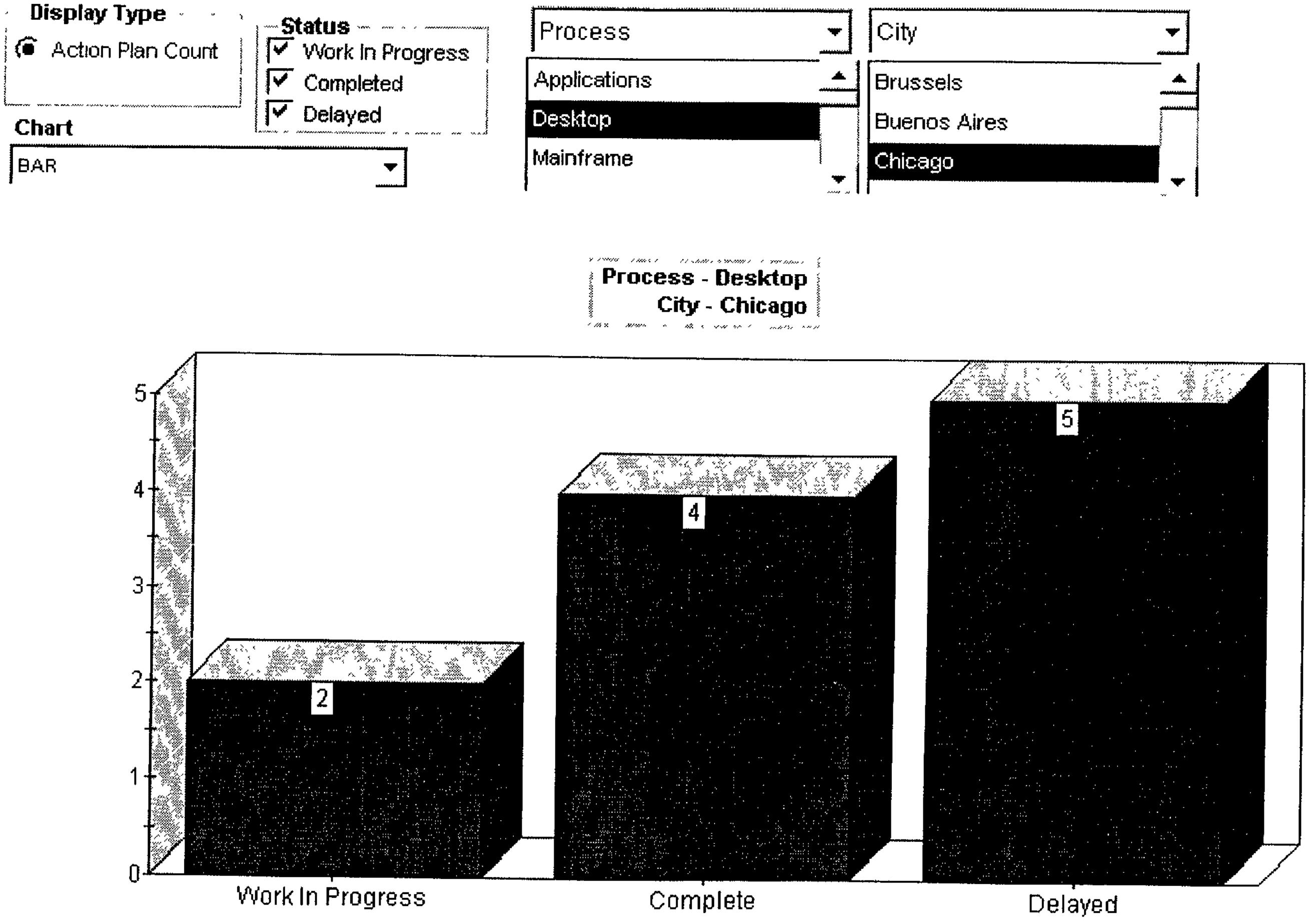


Report On Subrisk ▾ Bus Resum ▾ Detail For Overall ▾

Actuals vs Targets: Subrisk 'Bus. Resum.' (With Projected Target Scores)

09545391 . 041700

Fig 16



Display Type
● Action Plan Count

Status
☑ Work In Progress
☑ Completed
☑ Delayed

Chart
BAR

Process: Desktop (Applications, Desktop, Mainframe)

City: Chicago (Brussels, Buenos Aires, Chicago)

Process - Desktop
City - Chicago

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship is as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Method and System for Managing Risks

the specification of which (check only one item below)

[x] is attached hereto.

[ ] was filed as United States Application
on ____________________
Serial Number ________________
and was amended on ________________

[ ] was filed as PCT international application
on ____________________
Number ________________
and was amended on ________________

09545081 .040700

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 C.F.R. 1.56 (a).

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(b) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application on this invention filed me or my legal representatives or assignees and having a filing date before that of the application on which priority is claimed.

Foreign Application Number(s)	Country	Filing Date	Priority Claimed - (Yes or No)

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date

POWER OF ATTORNEY

As a named Inventor, I hereby appoint the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Attorney	Registration No.
Daniel A. DeVito	32,125
Edward V. Filardi	25,757
Constance S. Huttner	35,903
Robert B. Smith	28,538
Andrew F. Strobert	35,375
Jose Esteves	41,011
Guy Perry	46,194

09545381.040700

Send correspondence and direct telephone calls to:

Andrew F. Strobert
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Four Times Square
New York, NY 10036,
Telephone No. (212) 735-3000.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First Joint Inventor: Craig Spielmann

Inventor's signature: Craig R. Spielman Date signed: 3/30/00

Inventor Residence and Post Office Address:
162 Park Street
Montclair, NJ 07042
United States

Citizenship: United States

Full Name of Second Joint Inventor: Maria Hutter

Inventor's signature: Maria C. Hutter Date signed: 4/1/00

Inventor Residence and Post Office Address:
50 Reed Drive South
Princeton Junction, NJ 08550
United States

Citizenship: United States

09545381 . 040700

Full Name of Third Joint Inventor: Joel Klein

Inventor's signature: Joel Klein   Date signed: 3/31/00

Inventor Residence and Post Office Address:

27 Ridge Road
Croton, NY 10520
United States

Citizenship: United States

Full Name of Fourth Joint Inventor: Naresh Singhani

Inventor's signature: Naresh Singhani   Date signed: 3/31/00

Inventor Residence and Post Office Address:

375 Harrison Street
Paramus, NJ 07652
United States

Citizenship: United States